ACEEE *Proc. of Int. Conf.* on *Recent Trends in Information, Telecommunication and Computing, ITC*

Software Solution: Against Cold Boot Attack

Abhishek Kaushik[1] and Sudhanshu Naithani[2]
[1] Kiel University of Applied Science/Computer and Electrical Department, Kiel, Germany
Email: Abhishekkshk@gmail.com
[2] Nemi Chand Institute of Technology/Computer Science, Panipat, India
Email: naithanisudhanshu@gmail.com

***Abstract*— DRAM is an important memory of a computer. Microprocessor loads the data requested by the user into DRAM before processing the data. Hence, DRAM contains important information in a computer. Recently, researchers discovered that DRAM is vulnerable to attack that is called Cold boot attack. DRAM contents can be recovered even after the computer has been powered off for several minutes. The information obtained can be often use to break the disk encryption system such as File vault. In this paper, we proposed the methodology which explains the complete process and describe the safeguard methods. We design a system keeping few things in our mind the accessibility for the user and Security. This System is defines as a software solution to the cold boot problem. We also used additional feature to prevent DRAM from the machine replacement. The System is designed as the procedure to secure the encryption key and prevent the machine from attack.**

***Index Terms*— Coldboot attack, DRAM, Sensors, SSE Registers, Encryption keys, frozen cache**

I. INTRODUCTION

Your goal is to simulate the usual DRAM one of most essential part of memory that is being used by Computer .Most of People believe on the notion that the content in the DRAM is wiped away immediately after the power off to the System. In real view, the content of DRAM will persist for short period of time after the power being off. We can say the concept based on temperature and time. For some period of time, lower the temperature more will persistence time of Data in DRAM. [1, 2] .If temperature of DRAM is kept low, the data will remain in DRAM for some Minute or some hour's .This Phenomenal will provide an opportunity to a attacker to have an easy access to the System and the Memory .Some of the very famous Disk operating System including the popular Bit Locker used by Vista and File Vault used By Mac OS used to store the key information in DRAM after the access login. The Attacker can easily use the concept of cold boot attack to get access in the physical memory without using any device. By having the image of full memory and can access the encrypted key by the cold boot attack. Once the attacker gets the key, he/she can access all the content from memory. [1, 2]

So there is a software based solution of the cold boot attack. The main Concerns are security and flexibility of the System. Software should be platform independent and can have an easy access by the user.

The solution deals with multiple options such as temperature specified Storage, as temperature goes low the Dram automatically wiped away the content or System Specific DRAM means as DRAM can only work only on system specified and If we try it to another system ,the Dram will not be compatible and the data will

DOI: 02.ITC.2014.5.569
© Association of Computer Electronics and Electrical Engineers, 2014

be deleted. And we also had option to store the encrypted key into SSE registers rather than in DRAM. [3]
The Solution also deals with very high secure System. They use the methodology of Securing the key or encryption of the key. The main advantage of this method is that we don't have to use any extra registers or any special hardware configured device. The software just required few of the information regarding the system status, user login, software login and system information. So the encrypted key in the ram is protected by the complex password. The password consists of component that cannot be easily accessible by the attacker. And he/she can't access the entire component at the same time. It provides the unique secure system from the cold boot attack. [4]
Functional Description

1) Securing the Encryption key with the complex key.
2) Using the sensors in mother board for detection of temperature.
3) Deletions of the keys material being available after shut down.
4) Short keys directly stored as a plain text in registers.
5) It provides the dual Properties of storing the keys in DRAM or Registers. [1, 2, 3, 4 and 5].

II. How Cold Boot Attack Works

1) Cool the DRAM by spraying the inverted cans of "canned air" dusting spray on them.(fig.1)
2) Remove the DRAM from the Machine.
3) This process can maintain the data into DRAM for than 10 minutes

Figure 1: Cold boot attack, Spraying Duster into the chip and cooling the temperature up to – 50 Celsius

4) Then we can put the DRAM into the Coolant Machine.
5) The coolant Machine contains Nitrogen Liquid. That enables the DRAM to freeze.
6) By this we can keep DRAM Contain Data for weeks. It provides the flexibility to attacker in respect to time.
7) Now we can use DRAM for any machine.
8) Attacker can take the encryption key and other sensitive Data from DRAM and further used for the attack.[1, 2]

III. Previous Work

Cold Boot Attack has been a serious threat in last few years .Some of the computer scientist have suggested some suitable solution to prevent from the cold boot attack. As per the Frozen Cold Cache blog use of Full Encryption Software can prevent from cold boot attack.
According to the Blog, we can use CPU Cache instead of Dram to store the encryption key. The CPU cache is switched into special mode that enables the data to store in cache and unable to write in Ram. This is a convenient method to provide the safety from the cold boot attacks. [1, 5]
The main issue with the Frozen Cache is performance. This Solution restricts the performance of the System. As per the Suggestion by the author, this method is best to use when the Screen is locked. Secondly this method doesn't provide the security to the important content in the RAM. [1, 5]
Some computer Scientist focused on creating a secure environment for the execution. The latest example of the secure environment is SP (Secret Protected) Architecture and IBM Secure Coprocessor. The Secret Protected is an architecture that is purposed to protect the high sensitive data such as Password or Secret key In the Critical Execution mode, a Special Software Module is used to protect the user's secret key, the computation of secret keys and all the intermediate state and process are protected from observation and tempering by adversaries. This critical Execution mode is enabled to provide the secure execution with the

help of registers and cryptographic engines added to the general purpose processor. IBM4758 Secure Coprocessor is a machine which provides the secure software and hardware execution environment. [1, 6, 7] The architecture consists of three trust levels. The trust level is in the descending order from top to bottom. The hardware is most secure then firmware and software (fig. 2).While firmware more secure than software.

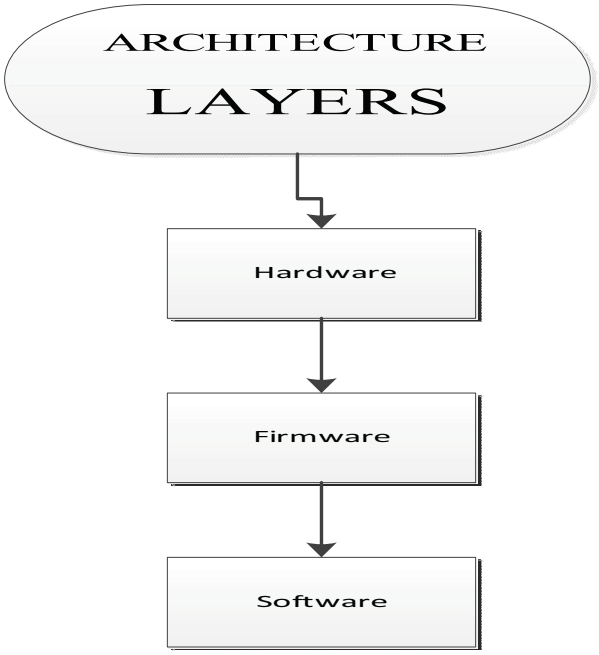

Figure 2: Architectural trust levels

The IBM 4758 Secure Coprocessor doesn't use slower software temper response instead of faster hardware temper response. The SP architecture and IBM4758 Coprocessor provide secure system securing the secret key. This system provides the proper authentications for the secure executions. However, SP architecture and IBM4758 Coprocessor need some changes on the current system and the architectures. This increases the manufacture cost of the current product. Generally, the hardware level protection is safer than a software-only solution which is easier to be attacked by the attacker. The Problem was the same that it doesn't provide the security to the Dram Content. [1, 6, 7]

IV. Characterizing The Remanence Effects

A DRAM is consists of the Capacitor. Each Capacitor cell encodes a single bit by either charging or not discharging cone of the capacitor's conductors. The other conductor is hard-wired either to power or to ground; depending on the cell's address within the chip [2, 8, 9, and 16] see fig. 3.

Figure 3: Dynamic Random Access memory

Capacitor property is to maintain the charge .Charge will leak out from the capacitor over some period of time. Capacitor will lose its value when it's discharged. So Capacitor must be recharged every time to hold or store the bits. Every DRAM Capacitor cell has fixed refreshed time. The standard refresh time is highly reliable for the normal operation of computer. A small bit error can cause a fatal error.
As it is high reliable, a failure to refresh any Dram capacitor cell within the time can hardly cause any probability of actually destroying the cell's content [2, 8, 9].

Figure 4: A picture of the Mona Lisa being recovered from system C's RAM at normal operational temperature of 20 to 25 °C after different amounts of time. Each picture's caption includes the percentage of correct bits that were recovered

We conducted a series of experiments to characterize. DRAM remanence effects and better understand the security properties of modern memories. We performed trials using PC systems with different memory technologies. These systems included models from several manufacturers and ranged in age from 9 years to 6 months. [2]

We test the remanence factor in two conditions. One is in the optimal condition (fig.4) and one is below optimal conditions in different models of memory. We find the significant change in the remanence properties. When we consider the case of the optimal temperature the error rate is very high of the data which we received from the Memory and in second case the error rate at below optimal temperature (-50 Celsius) is nearly not noticeable [2, 10, 11, 12, 13 and 14].

So we must keep those things in our mind while making the solution of the cold boot attack. Remanence effects are very important concepts for the cold boot attack and its related problems.

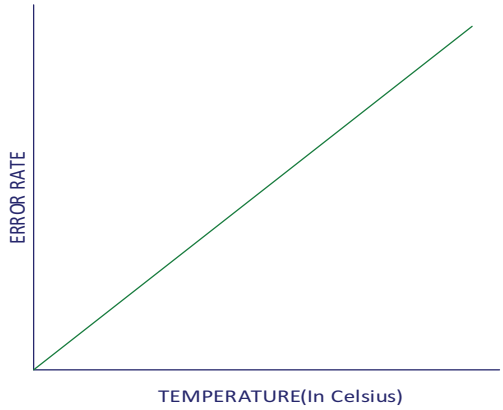

Figure 5: Its shows the relations between the temperature and the error rate

The given graph shows the relationship between the errors and the temperature (fig. 5). The error is defined comparison between the no of bits which is received after the cold boot attack and original values which is stored in respect of time. So temperature is directly propositional to the error. So temperature is less the error rate is less. According to cold boot attack, temperature is one of the most important factors of the remanence. The important factors for remanence are material of the memory, temperature and time. The material of semiconductor shows different properties of the graphs [2, 9, 10, 11, 12, 13 and 17].

V. Methodology

The main objective of this project is to implement the Software solution for the Cold Boot Attack. In order to achieve the goal, we need to design the system, implement and test it in the hardware.

Generally, the Software System can be divided into five phases.

They are:

1) Planning,
2) Design,

3) Software Implementation,
4) Hardware Implementation,
5) Results and discussion.
6) Advantage and disadvantage

A. Planning

Planning is the one of the important stage in the System. To produce the software based solution for the cold boot attack problem. The solution enables to provide the secure system from the cold boot attack. The main advantage of this system is that we don't require any extra device to store the encrypted key. The Software protected the encrypted key with the complex another AES 256 bit key length. The key consists of components that cannot easily accessible by the attacker. The key consists of four components such as the system status, user login, and software login and system information. It provides the unique secure system from the cold boot attack. We can also provide the option to keep the key in the CPU registers depending upon the length. [1, 2, 3, 4]

B. Design

Design is the core concepts of any of the solution. We design the given system in such way that it provides the unique solution of the cold boot attack problem. In the given design we used the concept of the Key protection and Temperature Specific. In the design system we have two options to store the encrypted key either in registers or in Dram depending upon the length of the key. if the length of the key is small it is directly save in registers as a plain text and if the length of key large enough then we will use the password oriented protection of the key (fig. 6) .We are also using temperature Specific sensors which are already in mother Board processor for the detections of the temperature. So if the temperature is below -25 Celsius. Then it's an alarm of misusing of the Dram .We can set up the algorithm to delete the Content when the temperature is below -25. [1, 2, 3, 4, 5, 6]

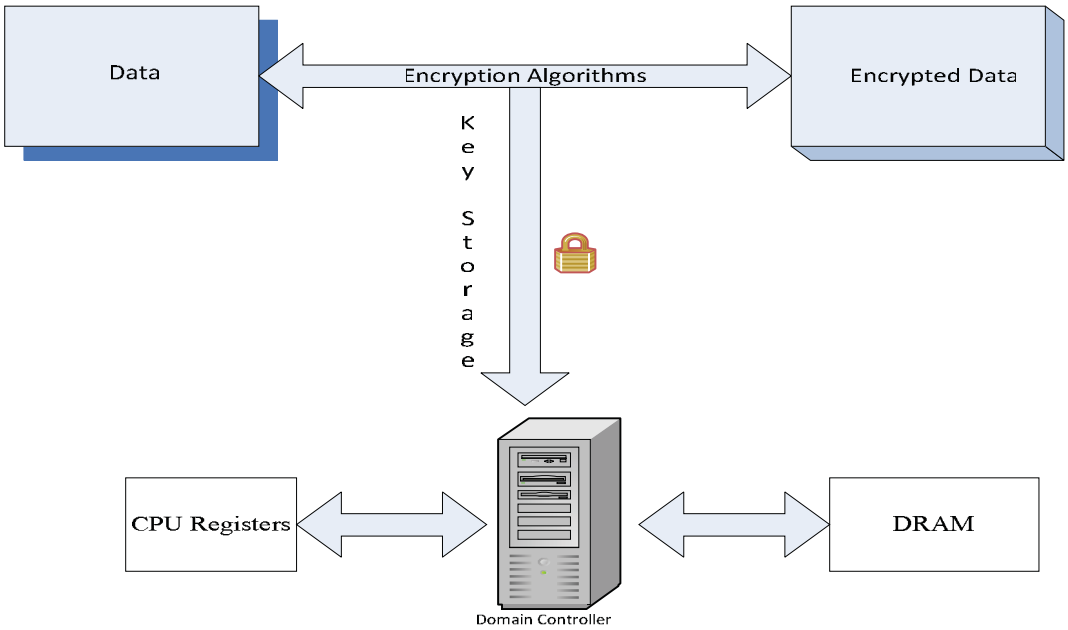

Figure 6: It shows that data is encrypted with algorithm (mostly AES) and key is kept either in DRAM or in CPU Registers (short keys). It totally depends upon the length of the key

C. Software Implementation

Software protects data on your laptop with centralized management from the Software Servers. Data never leaves your laptop and you do not need to be online to be protected

At its simplest, Software Solution consists of an agent on your laptop and the servers connected via the Internet (fig. 7). Software works whether you are online or offline and automatically checks into the servers when online. [4]

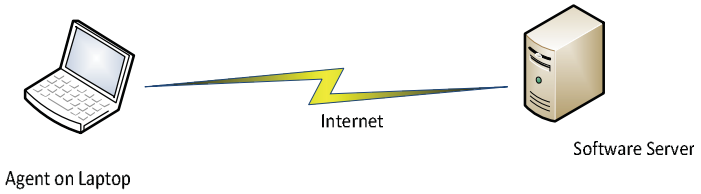

Figure 7: Its shows the Connection between server and agent Via Internet

i) The Agent manages:

1. Access and encryption of your data.
2. Security of your data against the attacker
3. Connection with the Software Server

ii) The Software Servers:

1. Manage and making of the Security policies
2. Keep the record of the access failure or entering the wrong password
3. Restoration of the computer access files
4. Actions taken on reports.
5. Restore the Software Access password

Software servers

a) Policy Management

We maintain the rules and policies for the agent. These policies are being designed while keeping the Security and usability in mind. These policy management is partially managed by the authenticate user. User can choose the policy under the standard conditions.

1) Users option about policies (user defined policies)

1. Change the Software password
2. Select the attempt of password failure before taking any actions
3. Select the durations to trigger the protective actions

2) Primitive policies

1. Discretely power to change password on the information(threat warning) from agent
2. Design new policies according to the requirement of the security level.
3. To define the policies scope (globally and locally)

b) Report a Computer Lost or Stolen and Restore the Access to Files

If a machine is being lost or stolen then the default action is to destroy the protection keys whenever machine will come online. User can also select an option of deleting the data. Especially data deletion is performed by the military purposes. And you can always recover it by the authentic user from the server. User can also reset the trigger of warning under the supervision of Server policies. [4][17]

The servers will automatically regenerate the data and enable access once the computer comes online if your computer has not been in use for many days.

c) Reporting

Software automatically collects the information on actions ordered from server and actions taken by machine. You can run a report that shows the logs. The logs contain the action of computer in respect to time and date. This also states the IP address and current status of the machine. [4][17]

In the software Implementations, We produce the solution to secure the encryption key. We Secure the Secret by encrypting the key. We must keep the Secret key in Machine itself to decrypt the data according to the requirement. Now the question arises how to protect the key. Most of the System protects the key with some password. But password can be guessed easily by cold boot attack. We provide the solution by securing the key in one of the most secure way. We can use any algorithm for the encryption (Depend upon the key length).We provide the solution which is extremely Complex password or key to protect the encryption key (fig. 8) .The protection key is of 256 bit AES key. As shown below, the 4 elements must be present to access the encryption key which allows you to open your files. [4]

The Four Elements

-Username: Software solution is user specific. Your data is only available to you. If an administrator or other user logs into your computer with their account they never have access to your data.

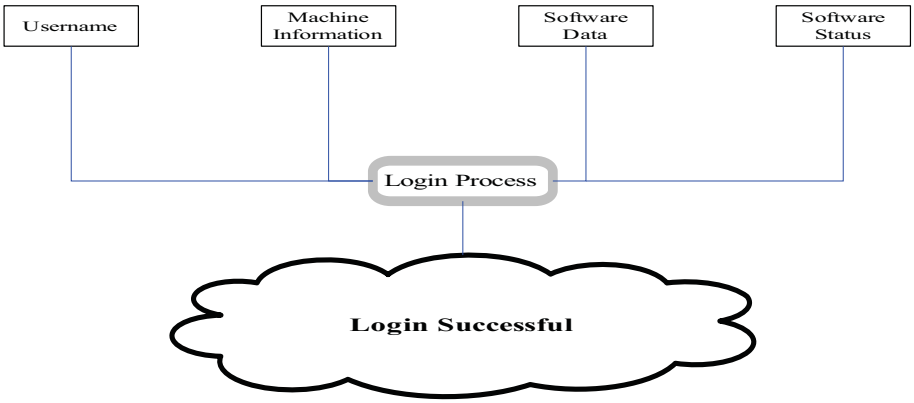

Figure 8: The encryption key is secured by the complex key .The User Name ,Machine Information ,Software Data and Software Status are combined together to form complex password

-Machine Information: Software automatically collect unique data from your computer as you are booting your computer. If the hard disk is moved to another computer, even an identical model, Software will not allow access to your data.

-Software Data: As discussed below, System Solution protects your data against different types of Attacks. That data is a set of information unique to your Software account that is deleted from your computer if a threat is sensed. Since this Software data is available on the Software servers, we can get it whenever we required.

-Software Status**:** This includes information indicating your computer registration Id and the Software registration id with your machine. This can only be access by the Software access password. [4]

iii) Software Access Password

The password is free from the encryption key and the protection key. If you login the password correctly, the Software status information is complete and correct. If you login with incorrect password you can't access your files. We also keep the record of your login failure. If the login failure is consecutive 5 failures then Server will block its Software Access Password .Then the User must contact to the server for the Software Access Password. [3] .We also programme the system so that it is temperature specific and if the temperature goes below certain limit we set up the programme to delete the data from DRAM. If the length of the key is small we can directly save into SSE registers. So it's the complete System which provides the unique solution for the latest threat of the cold boot attack. This also enables the system to be safe and secure. This also provides the protection against variety of attacks. We discussed in details in hardware Implementations. [4, 14]

D. Hardware Implementation

As far as the hardware Implementation we use temperature Sensors and SSE registers (key is small and depends upon the algorithm) to store the key.

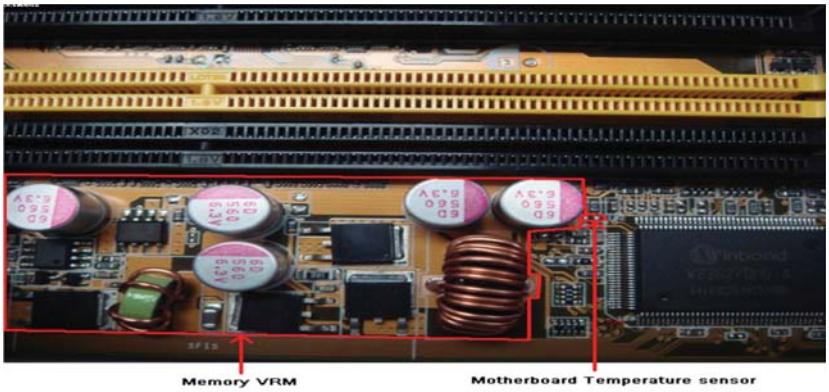

Figure 9: Shows mother board sensors

So we use the motherboard sensors for suspecting the attack. As soon as the temperature goes below the temperature limit, Our System will suspect the given temperature and take the necessary actions [15] (see fig. 9). It will be going to delete the content in the DRAM for the Safety Concern and will keep the copy of the content (Encryption key) in the Registers. This Module is the part of system protection from the attacker and it will not allow the user to access the DRAM after the physical control over the DRAM. [3, 4]
We can also store the encryption key as Plain text directly in the registers. It completely depends upon the key length of the encryption algorithm. Its complete an option according to the requirement. As the Storage in the Registers may influences the processing speed. It's an option to be used in critical situations. [3, 14]

E. Results and Discussions

In this section, we will discuss on the results of the architecture from our proposal. We included the complex password safety and use of the sensors that make the system unique and use of the SSE registers in critical situations. The proposal produces a very high secure System against cold boot attack

F. Advantages and Disadvantages

Our Solution prevents the data to be stored in the DRAM as clear text. And it provide the security against the laptop which being physically stolen and it also provide the system against any types of threats, it won't allow the any type of illegal access to the System.
The drawbacks of the proposal are reduced performance of the memory system and additional cost for implementing the Software solution. The concept of temperature specific and SSE Registers can't work in old Machine.

VI. CONCLUSION

As a conclusion, our proposal provides a good idea on defending against Cold Boot Attack. The design is a Software implementation which provides the Software and hardware level protection that is safer and better solution. The contents provide the security to the encryption key. It's not only providing the safety against cold boot attack but also from the other threats. Besides that, it also solves the current full disk encryption problems that store the key in the memory without requiring any change on the full disk encryption software .It provides the Secure encryption of data. It provides the protection against the hackers. It also blocks your computer and deletes the content from DRAM after suspecting of any illegal activities.

ACKNOWLEDGEMENT

With profound gratitude, we express our sincere thanks to everyone associated with us, directly or indirectly, during our rich experience with this project special thanks to Prof. Dr. Nils Gruschka (Kiel University of Applied Science, Germany) and Assit. Prof. Amit Kaushik (NC College of Information Technology, India) for their valuable advice and guidance that have helped us immensely in the successful completion of this project.

REFERENCES

[1] Joo Guan Ooi, Kok Horng Kam "A Proof of concept on defending cold boot attack", Intel Malaysia, September 2009
[2] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W.,Felten. "Lest We Remember: Cold Boot Attack on Encryption Keys", Princeton University, April 2008.
[3] Bit Armor: Bitarmor pdf blog 2008 http://www.highseclabs.com/ Resources/ BH_US_08_ McGregor_Cold_ Boot_Attacks.pdf
[4] Icelock:Blog on Icelock Mobile Security http://www.hyblue.com/icelock/MobileDataSecurity.aspx
[5] ACME Security, "Frozen Cache", http://frozencache.blogspot.com/, Jan 2009.
[6] R. Lee, P. Kwan, J.P. McGregor, J. Dwoskin, Z. Wang, "Architecture for Protecting Critical Secrets in Microprocessors", Proceedings of the 32nd International Symposium on Computer Architecture (ISCA 2005), pp. 2-13, June 2005.
[7] J. G. Dyer, M. Lindemann, R. Perez, R. Sailer, L. van Doorn, S. W. Smith, and S. Weingart, "Building the IBM 4758 secure coprocessor", IEEE Computer, v.34 n.10 p.57–66, 2001.
[8] SCHEICK, L. Z., GUERTIN, S. M., AND SWIFT, G. M. "Analysis of radiation effects on individual DRAMcells". IEEE Transactions on Nuclear Science 47 (Dec. 2000), 2534–2538.

[9] GUTMANN, P. Data remanence in semiconductor devices. In Proc. 10th USENIX Security Symposium (Aug. 2001), pp. 39–54.
[10] LINK, W., AND MAY, H.Eigenschaften von MOS-Ein-Transistorspeicherzellen bei tiefen Temperaturen. Archiv f¨ur Elek-tronik und ¨Ubertragungstechnik 33 (June 1979), 229–235.
[11] ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems, first ed. Wiley, Jan. 2001, p. 282.
[12] SMITH, S. W. Trusted Computing Platforms: Design and Appli- cations, first ed. Springer, 2005.
[13] WYNS, P., AND ANDERSON, R. L. Low-temperature operation of silicon dynamic random-access memories. IEEE Transactions on Electron Devices 36 (Aug. 1989), 1423–1428.
[14] Patrick Simmons" Security Through Amnesia: A Software-Based Solution to the Cold Boot Attack on Disk Encryption", 26 April 2011
[15] Figure 6: Mother board and its temperature Specific Sensors http://eservice.asus.com.tw/eService/eService /sShowImage?id=7992008B-09B0-CB9E-F460-A56CB98333C0.JPG
[16] Figure 3: Dynamic Random access memory and the Capacitor http://www.ktclear.in/techblog.php?tech_id= TECHNICAL%20TERMS:DRAM
[17] Icelock Quick pdf blog 2008 http://www.hyblue.com/icelock/IceLock_QuickStart.pdf